Discipline Specific Elective (DSE) Course - 4

Any *one* of the following (at least *two* shall be offered by the college):

DSE-4 (i): Number Theory
DSE-4 (ii): Linear Programming and Applications
DSE-4 (iii): Mechanics

DSE-4 (i): Number Theory

Total Marks: 100 (Theory: 75 and Internal Assessment: 25)
Workload: 5 Lectures, 1 Tutorial (per week) **Credits:** 6 (5+1)
Duration: 14 Weeks (70 Hrs.) **Examination:** 3 Hrs.

Course Objectives: In number theory there are challenging open problems which are comprehensible at undergraduate level, this course is intended to build a micro aptitude of understanding aesthetic aspect of mathematical instructions and gear young minds to ponder upon such problems. Also, another objective is to make the students familiar with simple number theoretic techniques, to be used in data security.

Course Learning Outcomes: This course will enable the students to:

i) Learn about some fascinating discoveries related to the properties of prime numbers, and some of the open problems in number theory, viz., Goldbach conjecture etc.
ii) Know about number theoretic functions and modular arithmetic.
iii) Solve linear, quadratic and system of linear congruence equations.
iv) Learn about public key crypto systems, in particular, RSA.

Unit 1: Distribution of Primes and Theory of Congruencies

Linear Diophantine equation, Prime counting function, Prime number theorem, Goldbach conjecture, Fermat and Mersenne primes, Congruence relation and its properties, Linear congruence and Chinese remainder theorem, Fermat's little theorem, Wilson's theorem.

Unit 2: Number Theoretic Functions

Number theoretic functions for sum and number of divisors, Multiplicative function, Möbius inversion formula, Greatest integer function. Euler’s phi-function and properties, Euler’s theorem.

Unit 3: Primitive Roots

The order of an integer modulo *n*, Primitive roots for primes, Composite numbers having primitive roots; Definition of quadratic residue of an odd prime, and Euler’s criterion.

Unit 4: Quadratic Reciprocity Law and Public Key Encryption

The Legendre symbol and its properties, Quadratic reciprocity, Quadratic congruencies with composite moduli; Public key encryption, RSA encryption and decryption.

References:

1. Burton, David M. (2012). *Elementary Number Theory* (7th ed.). Mc-Graw Hill Education Pvt. Ltd. Indian Reprint.

2. Jones, G. A., & Jones, J. Mary. (2005). *Elementary Number Theo*ry. Undergraduate Mathematics Series (SUMS). First Indian Print.

Additional Reading:

i. Neville Robinns. (2007). *Beginning Number Theory* (2nd ed.). Narosa Publishing House Pvt. Limited, Delhi.

Teaching Plan (DSE-4 (i): Number Theory):

Week 1: Linear Diophantine equation and its solutions, Distribution of primes, Prime counting function, Statement of the prime number theorem, Goldbach conjecture.

[1] Chapter 2 (Section 2.5).
[2] Chapter 2 (Section 2.2).

Week 2: Fermat and Mersenne primes, Congruence relation and its basic properties, Linear congruence equation and its solutions.

[2] Chapter 2 (Section 2.3).
[1] Chapter 4 (Sections 4.2 and 4.4).

Week 3: Chinese remainder theorem, to solve system of linear congruence for two variables, Fermat's little theorem, Wilson's theorem.

[1] Chapter 4 (Section 4.4), Chapter 5 (Section 5.2 up to before pseudo-prime at Page 90, Section 5.3).

Weeks 4 and 5: Number theoretic functions for sum and number of divisors, Multiplicative function, and the Möbius inversion formula. The greatest integer function, Euler's phi-function.

[1] Chapter 6 (Sections 6.1 to 6.2) and Chapter 7 (Section 7.2).

Week 6: Euler's theorem, Properties of Euler's phi-function.

[1] Chapter 7 (Sections 7.3 and 7.4).

Weeks 7 and 8: The order of an integer modulo *n*. Primitive roots for primes.

[1] Chapter 8 (Sections 8.1 and 8.2).

Week 9: Composite numbers having primitive roots.

[1] Chapter 8 (Section 8.3).

Week 10: Definition of quadratic residue of an odd prime, and Euler's criterion.

[1] Chapter 9 (Section 9.1).

Weeks 11 and 12: The Legendre symbol and its properties. Quadratic reciprocity law.

[1] Chapter 9 (Section 9.2 up to Page 181 and Section 9.3).

Week 13: Quadratic congruencies with composite moduli.

[1] Chapter 9 (Section 9.4).

Week 14: Public key encryption, RSA encryption and decryption scheme.

[1] Section 10.1.

Facilitating the Achievement of Course Learning Outcomes

Unit No.	Course Learning Outcomes	Teaching and Learning Activity	Assessment Tasks
1.	Learn about some fascinating discoveries related to the properties of prime numbers, and some of the open problems in number theory, viz., Goldbach conjecture etc.	(i) Each topic to be explained with examples. (ii) Students to be involved in discussions and encouraged to ask questions. (iii) Students to be given homework/assignments.	• Student presentations. • Participation in discussions. • Assignments and class tests. • Mid-term examinations.
2.	Know about number theoretic functions and modular arithmetic.		
3.	Solve linear, quadratic and system of linear congruence equations.		

4.	Learn about public key crypto systems, in particular, RSA.	(iv) Students to be encouraged to give short presentations.	• End-term examinations.

Keywords: Congruence, Decryption & Encryption, Legendre symbol, Multiplicative function, Prime numbers, Primitive roots, Reciprocity, Quadratic residue.